

1/5/5 (Item 5 from file: 351)
DIALOG(R) File 351:Derwent WPI
(c) 2004 Thomson Derwent. All rts. reserv.

011570706 **Image available**
WPI Acc No: 1997-547187/ 199750
XRPX Acc No: N97-456071

WWW gateway system for computer, network - has user management
communication unit to communicate with user management control unit which
forwards detection request from WWW gateway main body to management unit

Patent Assignee: HITACHI LTD (HITA)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 9265443	A	19971007	JP 9675863	A	19960329	199750 B

Priority Applications (No Type Date): JP 9675863 A 19960329

Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
JP 9265443 A 19 G06F-013/00

Abstract (Basic): JP 9265443 A

The system (7) has an user authentication information table (19) which matches and user authentication information input by a client with an user authentication identifier. The user authentication information is supplied based on an user authentication request. The user authentication information is detected based on detection request. An user authentication information management unit (17) deletes the authentication information which controls the access time for every user. An existing system enquiry unit (18) receives the user authentication information from the management unit. A WWW gateway communication unit (15) communicates with a WWW network. An user authentication request is sent to the existing system inquiry unit based on the user authentication information registration request received from the WWW gateway mainbody through the communication unit. The authentication information identifier acquires the authentication registration request for the management unit.

The authentication information request received from the network through the communication unit is forwarded to the management. An user management controller (13) forwards the deletion request received from the main body through the communication unit according to a communication break request from the user, to the management unit. An user management communication unit (14) communicates with the user management control unit for informing deletion request.

ADVANTAGE - Improves security of user authentication information.
Dwg.1/13

Title Terms: GATEWAY; SYSTEM; COMPUTER; NETWORK; USER; MANAGEMENT;
COMMUNICATE; UNIT; COMMUNICATE; USER; MANAGEMENT; CONTROL; UNIT; FORWARD;
DETECT; REQUEST; GATEWAY; MAIN; BODY; MANAGEMENT; UNIT

Derwent Class: T01

International Patent Class (Main): G06F-013/00

International Patent Class (Additional): G06F-001/00; G06F-015/00

File Segment: EPI

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-265443

(43)公開日 平成9年(1997)10月7日

(51)Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 13/00	3 5 7		G 0 6 F 13/00	3 5 7 Z
1/00	3 7 0		1/00	3 7 0 E
15/00	3 3 0		15/00	3 3 0 A

審査請求 未請求 請求項の数 3 O L (全 19 頁)

(21)出願番号 特願平8-75863

(22)出願日 平成8年(1996)3月29日

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 大高 政浩

神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア開発本部内

(72)発明者 橋本 和広

大阪府大阪市中央区北浜三丁目5番29号 日立西部ソフトウェア株式会社内

(72)発明者 小谷 純一

大阪府大阪市中央区北浜三丁目5番29号 日立西部ソフトウェア株式会社内

(74)代理人 弁理士 小川 勝男

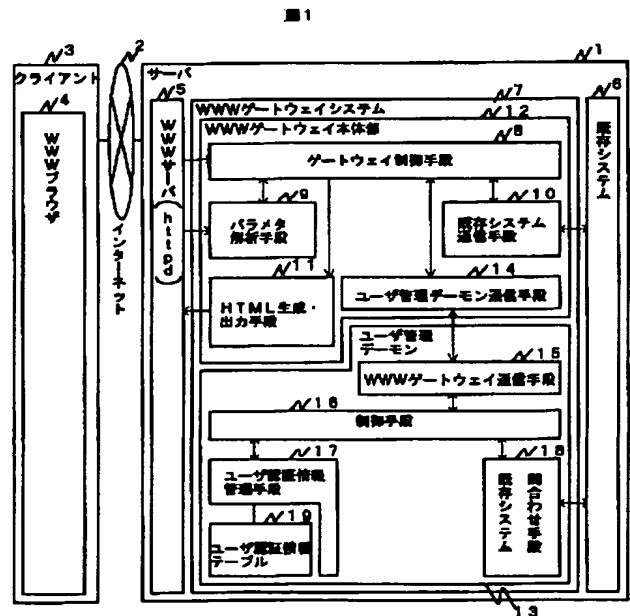
最終頁に続く

(54)【発明の名称】 WWWゲートウェイシステム

(57)【要約】

【課題】WWWゲートウェイプログラムのユーザ認証情報の画面間の継承がセキュリティホールとなる危険性がある点を解消し、セキュリティとユーザの利便性の両方を確保したユーザ認証によるアクセス権限管理が可能なWWWゲートウェイシステムを提供する。

【解決手段】WWWゲートウェイ本体部12における画面間のユーザ認証情報の継承をユーザ認証情報識別子をキーにして管理するユーザ認証情報管理手段17を備える計算機環境に常駐するユーザ管理デーモン13を有するものである。



【特許請求の範囲】

【請求項1】ユーザ認証情報登録要求に対してユーザがクライアントから入力したユーザ認証情報をユーザ認証情報識別子と対応付けて登録したユーザ認証情報テーブルと、ユーザ認証情報要求に対してユーザ認証情報を渡し、ユーザ認証情報削除要求に対し当該ユーザのユーザ認証情報を削除し、WWW（World Wide Web）ゲートウェイシステムに最後にアクセスした時刻をユーザ毎に管理し一定時間が経過したユーザのユーザ認証情報を削除するユーザ認証情報管理手段と、ユーザ認証要求に対してアクセス対象の既存システムにユーザがクライアントから入力したユーザ認証情報を渡し、ユーザ認証結果を受け取る既存システム間合わせ手段と、WWWゲートウェイ本体部との通信を行うWWWゲートウェイ通信手段と、

上記WWWゲートウェイ通信手段経由で受け取ったWWWゲートウェイ本体部からのユーザ認証情報登録要求に対して、ユーザ認証要求を上記既存システム間合わせ手段に発行し、その応答により認証成功ならばユーザ認証登録要求を上記ユーザ認証情報管理手段に発行して取得するユーザ認証情報識別子を、認証失敗ならば認証失敗通知を上記WWWゲートウェイ通信手段経由でWWWゲートウェイ本体部に応答し、また上記WWWゲートウェイ通信手段経由で受け取ったWWWゲートウェイ本体部からのユーザ認証情報要求を上記ユーザ認証情報管理手段に転送してその結果を上記WWWゲートウェイ通信手段経由でWWWゲートウェイ本体部に応答し、またユーザの通信断要求に応じて上記WWWゲートウェイ通信手段経由でWWWゲートウェイ本体部から受け取るユーザ認証情報削除要求を上記ユーザ認証情報管理手段に転送してその結果を上記WWWゲートウェイ通信手段経由でWWWゲートウェイ本体部に応答する制御手段を含むユーザ管理デーモンと、

WWWゲートウェイ本体部にユーザ管理デーモンとの通信を行うユーザ管理デーモン通信手段を備えたことを特徴とするWWWゲートウェイシステム。

【請求項2】請求項1に記載のWWWゲートウェイシステムにおいて、上記ユーザ管理デーモンとして、ユーザ情報テーブルを設け、ユーザ毎の情報を管理し、またWWWゲートウェイ本体部からの要求に対して当該情報を応答し、また上記ユーザ認証情報管理手段がユーザ認証情報を削除するときに当該ユーザのユーザ情報を上記ユーザ情報テーブルから削除するユーザ情報管理手段を備えたことを特徴とするWWWゲートウェイシステム。

【請求項3】請求項1に記載のWWWゲートウェイシステムにおいて、WWWゲートウェイ本体部として、上記ユーザ管理デーモンにユーザ認証情報要求をした結果、WWWゲートウェイシステムに最後にアクセスした

時間から一定時間が経過しておりユーザ認証情報が削除されている通知を受け取った場合に、表示するユーザ認証画面に前回の処理を継続するための情報を埋め込む継続処理情報埋め込み手段を備えたことを特徴とするWWWゲートウェイシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、WWW（World Wide Web）向けでない既存のシステムとWWWサーバの間を仲介して既存システムをWWWブラウザからアクセス可能にするWWWゲートウェイシステムに係わり、特にユーザ認証によるアクセス管理を行う既存システムに対して、当該システムのアクセス管理をそのまま活用するユーザ認証の手段を備えるWWWゲートウェイシステムに関する。

【0002】

【従来の技術】インターネット上に分散している資源を統一的にハイパーテキスト形式で参照（ブラウジング）するためのシステムであるWWWは、広域的な情報基盤として注目されている。このWWWを活用して既存のシステムに蓄積されている情報を全世界的に発信することを目的とした、既存システムとWWWサーバの間を仲介するゲートウェイプログラムの開発が盛んになっている（“特集／アプリケーション連携－業務プログラムもWWWで”、日経コミュニケーション12月18日号、第212号、1995年、136頁～140頁）。

【0003】WWWゲートウェイシステムは、CGI（Common Gateway Interface）スクリプトとして開発するのが一般的である。CGIはWWWサーバとサーバ上で動く他のプログラムやスクリプトとのインタフェースの役割を果たす（ローラ・リメイ：“続・HTML入門－新機能、CGI、Webの進化”、プレントイスホール出版、1995年）。

【0004】図2は従来のWWWゲートウェイシステムの構成を説明する図である。図2において、1はサーバ、3はクライアントであり、サーバ1とクライアント3はインターネット2で接続されている。サーバ1上ではWWWサーバ5（httpd：HyperText Transfer Protocol Daemon）を、クライアント3上ではWWWブラウザ4を動作させることにより、WWWによる情報発信および受信が可能になる。WWWゲートウェイシステム7は、WWWサーバ5から起動され、WWWサーバ5と既存システム6の仲介をする。

【0005】WWWゲートウェイシステム7は、WWWサーバ5からのデータの受信ならびにデータの解析を行うパラメタ解析手段9と、既存システム6とのインタフェースとなる既存システム通信手段10と、処理結果からWWWサーバ5向けの画面データ記述形式であるHTML（HyperText Markup Language）

3

age)形式で画面出力データを生成しWWWサーバ5に出力するHTML生成・出力手段11と、それらを制御するゲートウェイ制御手段8より構成される。ユーザからの処理要求をWWWブラウザ4からインターネット2経由で受け取ったWWWサーバ5は、それがWWWゲートウェイシステム7への処理要求ならばWWWゲートウェイシステム7を起動する。WWWゲートウェイシステム7では、パラメタ解析手段9がWWWサーバ5からデータを受け取り、解析し、それを基にゲートウェイ制御手段8が既存システム通信手段10を経由して既存システム6を操作して処理を行い、その結果をHTML生成・出力手段11によりHTML形式の画面データにしてWWWサーバ5に出力する。WWWサーバ5は、それをインターネット2を経由してクライアント3上のWWWブラウザ4に送信し、WWWブラウザ4がその画面データを表示する。以上のようにして、WWW向けでない既存システムをWWWを使用してアクセスできるようにする。

【0006】

【発明が解決しようとする課題】既存システムの中にはユーザ認証により情報に対するアクセス権限を管理する機能を持っているものがあり、WWWを通じて情報発信する際にもこのアクセス権限管理を有効にしたいとのニーズがある。そのためには、ゲートウェイプログラムがユーザからユーザIDやパスワードといったユーザ認証を行うための情報を入力させ、それを既存システムに渡すことが必要となる。しかし、WWWゲートウェイプログラムはゲートウェイプログラムを実現するCGIの仕様により、ユーザ操作のたびに起動され画面出力処理が終わるとプログラムの動作を終了しなければならず、ユーザの入力したユーザ認証情報に基づいて複数の画面を遷移して操作を行うような処理において、専用のクライアントアプリケーションのように既存システムとのセッションを接続したままにすることや、ユーザ認証情報をメモリ上に保持しつづけることができない。つまり、ユーザ認証情報の画面間の継承が問題となる。

【0007】この問題に対する一般的な解決方法としては、HTMLのhiddenタグを使用して画面情報にユーザ認証情報を埋め込む方法と、画面毎に必要な応じてユーザ認証情報を再入力させる方法の2つの方法が考えられる。しかし、前者では、例えば画面情報に埋め込んだユーザ認証情報を暗号化したとしても、画面情報のハッキングによりセキュリティホールとなる危険性がある。後者では、ユーザ認証情報を度々入力しなければならず、ユーザの利便性を著しく損なうこととなる。

【0008】本発明の目的は、ユーザ認証によるアクセス管理を行う既存システムに対して、ユーザの入力したユーザ認証情報に基づいて複数の画面を遷移して操作を行うような処理において、ユーザ認証情報の画面間の継承を行うことにより、セキュリティとユーザの利便性

4

(アクセスのたびにユーザ認証情報を入力しなくて良い)の両方を確保したWWWゲートウェイシステムを提供することにある。

【0009】

【課題を解決するための手段】ユーザ認証情報を計算機環境に常駐するユーザ管理デーモンに管理させ、WWWゲートウェイ本体部(以下では、WWWゲートウェイシステムを従来のWWWゲートウェイシステムとユーザ管理デーモンを統合したものと位置付け、従来のWWWゲートウェイシステムはWWWゲートウェイ本体部と呼ぶ)はそこから取得したユーザ認証情報を使用することにより、前記課題を解決する。ユーザ管理デーモンはユーザ認証情報毎にユニークでかつハッキングのされにくいユーザ認証情報識別子を割り振り、それをWWWゲートウェイ本体部に渡す。WWWゲートウェイ本体部はユーザ認証情報の代わりにユーザ認証情報識別子を画面間で継承し、ユーザ認証情報が必要な場合はユーザ認証情報識別子をキーにユーザ管理デーモンにユーザ認証情報要求を発行してユーザ認証情報を取得する。以上のようにユーザ管理デーモンにユーザ認証情報を管理させることにより、セキュリティとユーザの利便性の両方を確保したユーザ認証情報の画面間の継承が可能となる。

【0010】ユーザ管理デーモンは、具体的には次の手段で構成する。

【0011】(1)ユーザ認証情報テーブルを設け、ユーザ認証情報登録要求に対してユーザがクライアントから入力したユーザ認証情報をユーザ認証情報識別子と対応付けて登録し、またユーザ認証情報要求に対してユーザ認証情報を渡し、またユーザ認証情報削除要求に対し当該ユーザのユーザ認証情報を削除し、またWWWゲートウェイシステムに最後にアクセスした時刻をユーザ毎に管理し一定時間が経過したユーザのユーザ認証情報を削除するユーザ認証情報管理手段

(2)ユーザ認証要求に対してアクセス対象の既存システムにユーザがクライアントから入力したユーザ認証情報を渡し、ユーザ認証結果を受け取る既存システム間合わせ手段

(3)WWWゲートウェイ本体部との通信を行うWWWゲートウェイ通信手段

(4)上記WWWゲートウェイ通信手段経由で受け取ったWWWゲートウェイ本体部からのユーザ認証情報登録要求に対して、ユーザ認証要求を上記既存システム間合わせ手段に発行し、その応答により認証成功ならばユーザ認証登録要求を上記ユーザ認証情報管理手段に発行して取得するユーザ認証情報識別子を、認証失敗ならば認証失敗通知を上記WWWゲートウェイ通信手段経由でWWWゲートウェイ本体部に応答し、また上記WWWゲートウェイ通信手段経由で受け取ったWWWゲートウェイ本体部からのユーザ認証情報要求を上記ユーザ認証情報管理手段に転送してその結果を上記WWWゲートウェイ

通信手段経由でWWWゲートウェイ本体部に応答し、またユーザの通信断要求に応じて上記WWWゲートウェイ通信手段経由でWWWゲートウェイ本体部から受け取るユーザ認証情報削除要求を上記ユーザ認証情報管理手段に転送してその結果を上記WWWゲートウェイ通信手段経由でWWWゲートウェイ本体部に応答する制御手段また、WWWゲートウェイ本体部にもユーザ管理デーモンとの通信を行うユーザ管理デーモン通信手段を追加する。

【0012】これらの手段をWWWゲートウェイシステムに付加し、ユーザ管理デーモンを計算機環境に常駐させることにより、ユーザ認証情報はユーザ管理デーモンの作業メモリ上に管理し、画面間のユーザ認証情報の継承はユーザがWWWゲートウェイシステムへのアクセスを開始するたびに設定されるユーザ認証情報識別子により行われるようになり、セキュリティとユーザの利便性の両方を確保したユーザ認証情報の画面間の継承が可能となる。

【0013】

【発明の実施の形態】以下、本発明の実施の形態について例を上げて詳細に説明する。

【0014】まず第1の実施例について説明する。

【0015】図1は本実施例の構成を示すブロック図である。図1において、1はサーバ、2はインターネット、3はクライアント、4はWWWブラウザ、5はWWWサーバ、6は既存システム、7はWWWゲートウェイシステムである。ここで、WWWゲートウェイシステム7は、WWWゲートウェイ本体部12とユーザ管理デーモン13よりなる。

【0016】WWWゲートウェイ本体部12は、WWWサーバ5から起動される部分である。WWWゲートウェイ本体部の実装には、WWWサーバ5とのインタフェースを提供するCGIを導入しても良い。WWWゲートウェイ本体部12は、WWWブラウザ4上でユーザがした画面操作（例えばボタン押下やアンカークリック）に対してWWWサーバ5により起動され、一連の処理を行った後、画面データをWWWサーバ5に対して出力して動作を終了する。一方、ユーザ管理デーモン13はWWWゲートウェイ本体部12が起動される前にシステム管理者が起動し、システム管理者が明示的に停止させるまで計算機環境上に常駐し続ける。そしてWWWゲートウェイ本体部12からの処理要求を受け、それに対して応答する。

【0017】WWWゲートウェイ本体部12は、従来のWWWゲートウェイの要素であるゲートウェイ制御手段8と、パラメタ解析手段9と、既存システム通信手段10と、HTML生成・出力手段11と、それに加えてユーザ管理デーモン通信手段14より構成する。ユーザ管理デーモン通信手段14は、ゲートウェイ制御手段8からの通信処理要求に対してユーザ管理デーモン13に発

行するメッセージを生成して発行し、またユーザ管理デーモン13から受け取った応答をゲートウェイ制御手段8で処理できるかたちに変換する機能を持つ。

【0018】ユーザ管理デーモン13は、WWWゲートウェイ本体部12との通信を制御するWWWゲートウェイ通信手段15と、ユーザ認証情報を格納するユーザ認証情報テーブル19と、ユーザ認証情報テーブル19を管理するユーザ認証情報管理手段17と、既存システム6に対してユーザ認証の判定要求を発行する既存システム問合わせ手段18と、以上のユーザ管理デーモン13の構成要素を制御する制御手段16より構成する。

【0019】ここでユーザ認証情報テーブル19に格納するユーザ認証情報とは、既存システム6がユーザ認証を行うために要求する情報であり、例えば各ユーザ毎に割り振られたユーザIDやパスワードであってもよい。

【0020】図3は、ユーザ認証情報テーブル19の例を説明するための図である。この例ではユーザ認証のための情報として、ユーザIDとパスワードとIPアドレスを使用している。これらのユーザ認証情報にアクセスするためのキーとして各情報にユーザ認証情報識別子を付加する。ユーザ認証情報識別子は、ユーザ認証情報を取得するためのキーとして使用されるため、ユニークでなければならない。また、WWWゲートウェイ本体部12に渡され、画面情報に埋め込んで継承されるため、盗用される恐れのないものでなければならない。例えば、当該ユーザのユーザIDと、当該ユーザがWWWゲートウェイシステム7の操作を開始した日時と、起動されたWWWゲートウェイ本体部12のプロセスIDについて、末尾を予め定めたサイズだけ切り出して連結し、それを予め定めた手順で暗号化して生成した文字列をユーザ認証情報識別子として使用しても良い。ユーザ認証情報テーブル19はさらに当該ユーザが最後にWWWゲートウェイシステム7にアクセスした時刻を格納するフィールドも含む。これは、WWWゲートウェイシステム7に一定時間アクセスがなかった場合に当該ユーザの認証情報を削除する処理（タイムアウト処理）で使用される。

【0021】なお、ユーザ認証情報テーブル19をファイルとして管理するとそれを参照して盗用される恐れがあるため、ユーザ認証情報テーブル19はユーザ管理デーモン13が管理する作業メモリ上に管理する。

【0022】図1の構成のWWWゲートウェイシステム7でユーザの操作に対する処理の流れを次に説明する。

【0023】ユーザがWWWゲートウェイシステム7にアクセスすると、WWWゲートウェイシステム7はまずユーザ認証情報を入力するための画面（以下ではユーザ認証画面と呼ぶ）を表示してユーザにユーザ認証情報の入力を促す。WWWゲートウェイシステム7を使用して既存システム6にアクセスするためには、ユーザはまずユーザ認証画面でユーザ認証情報を入力しなければなら

7

ない。図4にユーザがユーザ認証画面でユーザ認証情報を入力したとき（この操作を以下ではログインと呼ぶ）のWWWゲートウェイシステム7の処理の流れを示す。

【0024】ユーザがログインをするとWWWサーバ5がWWWゲートウェイ本体部12を起動する。WWWゲートウェイ本体部12ではゲートウェイ制御手段8が処理101においてパラメタ解析手段9にパラメタ解析要求201を発行する。パラメタ解析手段9は、処理102においてWWWサーバ5からパラメタを入力しそれを解析してゲートウェイ制御手段8に応答する（202）。パラメタ解析結果202を受け取ったゲートウェイ制御手段8は、解析結果からユーザの操作がユーザ認証情報入力であることを判断して、処理103においてユーザ認証要求203をユーザ管理デーモン通信手段14に発行する。ユーザ管理デーモン通信手段14は、処理104においてユーザ認証要求203をユーザ管理デーモン13に対するメッセージ204に変換し、それをユーザ管理デーモン13に発行する。そしてユーザ管理デーモン13からの応答待機状態に遷移する。

【0025】ユーザ管理デーモン通信手段14が発行したメッセージ204はユーザ管理デーモン13の中のWWWゲートウェイ通信手段15が受け取る。WWWゲートウェイ通信手段15は処理105において受け取ったメッセージ204を解析しその結果を制御手段16に送信する（205）。メッセージ解析結果205を受け取った制御手段16は、処理106において解析結果からユーザ認証情報を取り出しそれをもとにユーザ認証要求206を既存システム問合わせ手段18に発行する。ユーザ認証要求206を受け取った既存システム問合わせ手段18は、処理107においてそれを既存システム6向けの処理要求207にして既存システム6へ発行する。既存システム6は受け取ったユーザ認証情報からユーザ認証を行い、当該ユーザが既存システム6にアクセスできるかどうかの判定結果を既存システム問合わせ手段18に応答する（208）。このように、ユーザ認証画面を表示しユーザ認証情報を受け取るのはWWWゲートウェイシステム7だが、WWWゲートウェイシステム7自体がアクセス権限管理を行うわけではなく、既存システム6にユーザ認証情報を渡して既存システム6がユーザ認証によるアクセス権限管理を行う。

【0026】既存システム6からユーザ認証結果208を受信した既存システム問合わせ手段18は、処理108においてそのユーザ認証結果209を制御手段16に応答する。制御手段16は、処理109において認証結果209の判定を行う。もし当該ユーザが既存システム6にアクセス可能であるという認証結果ならば、そのユーザ認証情報をユーザ認証情報テーブル19に登録するようユーザ認証情報管理手段17に処理要求210を発行する。ユーザ認証情報登録要求210を受けたユーザ認証情報管理手段17は、まず処理110でユーザ認証

8

情報識別子を生成する。ユーザ認証情報識別子の生成には上記で説明した、WWWゲートウェイ本体部12からのメッセージで渡されるユーザIDやプロセスID、ユーザ管理デーモンが独自に取得する操作開始時刻を結合し暗号化する方法を使用してもよい。処理110でユーザ認証情報識別子を生成した後、処理111でそのユーザ認証情報識別子とユーザ認証情報、およびアクセス時刻をユーザ認証情報テーブル19に格納する。ユーザ認証情報管理手段17は、当該ユーザ認証情報をユーザ認証情報テーブル19に格納した後、制御手段16にユーザ認証情報識別子を応答する（211）。応答211を受け取った制御手段16は処理112としてユーザ認証情報識別子をWWWゲートウェイ本体部12に応答するようWWWゲートウェイ通信手段15に処理要求を発行する（212）。

【0027】一方、処理109で当該ユーザが既存システム6にアクセスできないという認証結果ならば、制御手段16は上記の処理110と処理111のユーザ認証情報の登録は行わず、処理112においてユーザ認証に失敗した旨をWWWゲートウェイ本体部12に応答するようWWWゲートウェイ通信手段15に処理要求を発行する（212）。

【0028】WWWゲートウェイ通信手段15は、処理113において制御手段16から受け取った処理結果をWWWゲートウェイ本体部12に発信するメッセージ213に変換し、それをWWWゲートウェイ本体部12に発信する。以上でユーザ管理デーモン13の一連の処理は終了するが、ユーザ管理デーモン13は動作を停止せずに、計算機環境に常駐しWWWゲートウェイ本体部12からの処理要求待機状態に遷移する。

【0029】WWWゲートウェイ通信手段15が発行したメッセージは、ユーザ管理デーモン13からの応答待機状態にあったユーザ管理デーモン通信手段14が受け取り、処理114においてそれを解析してゲートウェイ制御手段8に送信する（214）。メッセージ解析結果214を受け取ったゲートウェイ制御手段8は、処理115においてユーザ認証結果を表示する画面情報（HTML形式）の出力要求215をHTML生成・出力手段11に発行する。このとき、ユーザ管理デーモン13から受け取ったユーザ認証結果がユーザ認証成功、すなわちユーザ認証情報識別子ならばそれを埋め込んだシステムの初期画面の画面情報の生成を指示し、ユーザ認証失敗通知ならばユーザ認証に失敗したことをユーザに通知し再度ユーザ認証情報を入力させるための画面情報の生成を指示する。

【0030】画面情報の出力要求215を受け取ったHTML生成・出力手段11は、まず処理116において画面情報を生成し、その画面情報を処理117においてWWWサーバ5に出力する（216）。ユーザ認証情報識別子の画面情報への埋め込みには、HTMLのhid

denタグを使用する方法を採用する。以上でWWWゲートウェイ本体部12の一連の処理が終了し、WWWゲートウェイ本体部12は動作を停止する。

【0031】ユーザがログインすると、WWWゲートウェイシステム7では既存システム6に当該ユーザ認証情報を渡してユーザ認証によるアクセス権限の確認を行わせた後、もし当該ユーザが既存システム6にアクセス可能ならば、当該ユーザ認証情報をユーザ管理デーモン13のユーザ認証情報テーブル19に登録する。そして、ユーザ認証情報テーブル19から当該ユーザ認証情報を取り出すためのキーとなるユーザ認証情報識別子をWWWゲートウェイ本体部12が出力する画面情報に埋め込み画面間のユーザ認証情報の継承を行う。

【0032】次に画面情報に埋め込まれたユーザ認証情報識別子を基にユーザ認証情報を取得し既存システム6にアクセスするときの処理の流れを説明する。

【0033】図5は、WWWゲートウェイシステム7からユーザ認証の必要な既存システム6の処理を実行するときの処理の流れを説明する図である。

【0034】上記と同様にパラメタ解析手段9の解析結果202を受け取ったゲートウェイ制御手段8が、解析結果202を基にWWWゲートウェイ本体部12の実行すべき処理を決定する。本実施例では、ユーザ認証の必要な既存システム6の処理を実行するものとする、ゲートウェイ制御手段8はまず前画面に埋め込まれていたユーザ認証情報識別子をパラメタ解析手段9の解析結果から取り出し、それをキーにしてユーザ管理デーモン13からユーザ認証情報を取得する。そのために処理121において、ユーザ認証情報要求221をユーザ管理デーモン通信手段14に送信する。

【0035】ユーザ管理デーモン通信手段14では上記と同様にゲートウェイ制御手段8から受けたユーザ管理デーモン13への処理要求221をメッセージ204に変換し、ユーザ管理デーモン13に発信する。ユーザ管理デーモン13では、WWWゲートウェイ通信手段15が当該メッセージを受信し、解析を行ない、その結果205を制御手段16に送信する。制御手段16は、処理122において解析結果205からユーザ認証情報識別子を取り出し、それをキーにして求めるユーザ認証情報を検索するよう、ユーザ認証情報管理手段17にユーザ認証情報要求222を送信する。ユーザ認証情報管理手段17は、処理123においてユーザ認証情報要求222からユーザ認証情報識別子を取り出し、それをキーにしてユーザ認証情報テーブル19の検索を実行する。

【0036】例えば、図3のユーザ認証情報テーブル19の例において、ユーザ認証情報識別子KUI03890V93が与えられたとすると、それに対するユーザ認証情報として、ユーザID:AIKOU、パスワード:ZZZ&&()@、IPアドレス:123.45.67.123を取得する。この際、テーブルにアクセスし

た時刻で最終アクセス時間のフィールドを置き換える。例えば、テーブルにアクセスした時刻が960308173247だとすると、現在登録されている最終アクセス時刻:960308154517を960308173247に置き換える。取得したユーザ認証情報を制御手段16に応答する(223)。なお、ユーザ認証情報管理手段17において当該ユーザ認証情報識別子に対応した情報がユーザ認証情報テーブル19に存在しない場合は、エラーを出力する。

10 【0037】ユーザ認証情報を受け取った制御手段16は、上記の例と同様にその結果をWWWゲートウェイ通信手段15経由でWWWゲートウェイ本体部12に応答し、応答メッセージを受け取ったユーザ管理デーモン通信手段14がそれを解析してWWWゲートウェイ制御手段8に渡す。

【0038】ユーザ管理デーモン13からのメッセージの解析結果としてユーザ認証情報を受け取ったゲートウェイ制御手段8は、それを付加した既存システム6への処理要求224を既存システム通信手段10に発行する。処理要求224を受け取った既存システム通信手段10は、処理125において既存システム6向けの処理要求225を生成して発行する。処理要求225を受け取った既存システム6は、処理要求225に含まれたユーザ認証情報によるアクセス権限に基づいた処理を実行しその結果をWWWゲートウェイ本体部12に応答する。以降は従来のWWWゲートウェイシステムと同様に処理結果からHTML形式の画面情報を生成し、それをWWWサーバ5に出力して一連の処理を終了する。ただし、出力する画面情報にはユーザ認証情報識別子を継承する。

30 【0039】以上のように、画面情報の中にユーザ認証情報識別子を埋め込み、それをWWWゲートウェイ本体部12のパラメタ解析手段9により取り出し、それをキーにしてユーザ管理デーモン13のユーザ認証情報管理手段17から当該ユーザのユーザ認証情報を取得し、それに基づいた処理依頼を既存システム6にすることにより、WWWゲートウェイシステム7からユーザ認証の必要な既存システム6の処理を実行することが可能となる。処理の実行結果として出力する画面情報に、またユーザ認証情報識別子を埋め込むことにより、次のWWWゲートウェイシステム7の起動にユーザ認証情報を継承することができる。

40 【0040】以上のようにしてユーザ管理デーモン13の中のユーザ認証情報テーブル19にユーザ認証情報を蓄積し、それにユーザ認証情報識別子をキーにしてアクセスすることにより画面間でユーザ認証情報を継承する。しかし、ユーザ認証情報を格納しつづけるとユーザ認証情報テーブル19のメモリサイズが増大し、ひいては計算機環境のリソース不足を招くことになる。よって、ユーザ認証情報テーブル19からユーザ認証情報を

削除する処理が必要となる。ユーザ認証情報テーブル19からユーザ認証情報を削除する手順として、次に2つの手順を説明する。

【0041】第1の手順は、ユーザから明示的にWWWゲートウェイシステム7の利用終了を通知させる（以下ではこの操作をログアウトと呼ぶ）ものである。画面にユーザがログアウトするための部品を用意し、それに対して操作されたときにユーザ認証情報管理手段17がユーザ認証情報テーブル19から当該ユーザのユーザ認証情報を削除する。

【0042】しかし、第1の手順だけでは、ユーザがログアウトし忘れた場合などにユーザ認証情報がユーザ認証情報テーブル19に残ったままになってしまう。WWWブラウザ4は、表示した画面をキャッシュしておき、画面操作でWWWブラウザ4起動時から表示してきた画面を順次再表示する機能を持っている。ユーザがWWWブラウザ4でハイパーリンクをたどって次々に画面遷移していくうちに、WWWゲートウェイシステム7をログアウトし忘れることが起こり得るが、このとき第3者が上記の画面キャッシュの機能により、WWWゲートウェイシステム7の画面を再表示し操作すると、ユーザ認証に必要なユーザ認証情報識別子が画面に埋め込まれているため、当該ユーザの権限で第3者の不正な操作を受け付けてしまうこととなる（ログアウト後は、既にユーザ認証情報識別子に対応したユーザ認証情報テーブル19の項目が削除されているため、画面キャッシュの機能でゲートウェイシステム7の画面を再表示し操作しても有効にならない）。

【0043】こうした問題を軽減する第2の手順として、ユーザがWWWゲートウェイシステム7に最後にアクセスした時刻から予め定められた時間が経過したユーザの認証情報をユーザ認証情報テーブル19から削除する（こうしたユーザ管理デモン13の処理を以下ではタイムアウト処理と呼ぶ）。図3の例に示した通り、ユーザ認証情報テーブル19の各項目に対して最終アクセス時刻を設定するフィールドを用意する。

【0044】上記の説明でも触れたとおり、WWWゲートウェイシステム7にアクセスするたびにユーザ管理デモン13のユーザ認証情報管理手段17が当該ユーザの最終アクセス時刻を更新する。ユーザ認証情報管理手段17は、最終アクセス時刻を監視し、アクセスされないまま最終アクセス時刻から予め定義された時間が経過した項目を自動的に削除する。こうすることにより、ユーザがログアウトし忘れた場合にユーザ認証情報がユーザ認証情報テーブル19に残ってしまうという問題を解消できる。タイムアウト処理によりユーザ認証情報を削除されたユーザがWWWゲートウェイシステム7にアクセスした場合には、再度ユーザ認証画面を表示しユーザ認証情報を入力させる。

【0045】以上のように、ユーザの操作によりWWW

サーバ5から起動され、一連の処理が終了した時点で動作を停止するWWWゲートウェイ本体部12に対して、システム管理者が起動し計算機環境に常駐し続けるユーザ管理デモン13にユーザ認証情報を管理させ、WWWゲートウェイ本体部12は画面情報に埋め込まれたユーザ認証情報識別子をキーとしてユーザ認証情報を取得することにより、画面間でユーザ認証情報を継承でき、またユーザ認証情報識別子としてユニークでかつハッキングしにくいIDを定義することで、セキュリティとユーザの利便性の両方が高いアクセス権限管理の可能なWWWゲートウェイシステムを実現することが可能となる。

【0046】また、ユーザがログアウトにより明示的にWWWゲートウェイシステムの利用終了を通知したときに当該ユーザのユーザ認証情報をユーザ認証情報テーブルから削除する手順と、ユーザ管理デモンが最終アクセス時刻からの経過時間を監視し、タイムアウト処理で一定時間アクセスのなかったユーザのユーザ認証情報をユーザ認証情報テーブルから削除する手順を用意することにより、ユーザ認証情報の追加登録によるユーザ認証情報テーブルの肥大化とWWWブラウザの画面キャッシュ機能を悪用した第3者による既存システムへの不正アクセスを防止することが可能となる。

【0047】次に第2の実施例について説明する。

【0048】上記第1の実施例では、ユーザ管理デモンはユーザ認証情報のみを管理した。しかし、ユーザ管理デモンにその他の情報を管理させることも可能である。ユーザ管理デモンに管理させることが有効な情報としては、ユーザ毎に管理すべき情報であり、かつ画面間で継承する必要がある情報があげられる。

【0049】例としては、既存システムに渡すべきコンフィギュレーションパラメタなどが考えられる。画面間で継承する必要がある情報は通常画面情報に埋め込んで継承するが、WWWブラウザで参照できてしまう画面情報に埋め込むことがセキュリティの観点から適切でない情報の継承に特に有効である。

【0050】図6は本実施例の構成を示すブロック図である。図において、ユーザ管理デモン13にユーザ毎に追加情報を格納するユーザ情報テーブル21とそれを管理するユーザ情報管理手段20を追加する。

【0051】図7は本実施例におけるユーザ認証情報テーブル19の例である。各ユーザ毎にユーザ情報テーブルへのアドレスを格納するためのフィールドを追加している。図8は本実施例におけるユーザ情報テーブル21の例である。ユーザ認証情報テーブル19に登録されたアドレスに既存システム6に渡すコンフィギュレーションパラメタが2つ格納されている。

【0052】図9で本実施例におけるログイン時のWWWゲートウェイシステム7の処理の流れを説明する。ユーザ管理デモン13の既存システム問合わせ手段18

の結果に対して制御手段 1 6 で認証結果判定 1 0 9 を行うまでの処理は、第 1 の実施例におけるログイン時の処理(図 4)と同じである。また、認証結果判定 1 0 9 で認証失敗と判定した場合の以降の処理もまた第 1 の実施例におけるログイン時の処理と同じである。認証結果判定 1 0 9 において認証成功と判定した場合、既存システム問合わせ手段 1 8 に対してユーザ情報要求 2 3 1 を発行する。既存システム問合わせ手段 1 8 は、処理 1 3 1 においてそれを既存システム向けのユーザ情報要求 2 3 2 に変換して発行する。既存システム 6 ではユーザ情報を検索してそれを応答する(2 3 3)。既存システム 6 からユーザ情報の応答 2 3 3 を受けた既存システム問合わせ手段 1 8 は、処理 1 3 2 においてそれを制御手段 1 6 に応答する(2 3 4)。

【0 0 5 3】既存システム問合わせ手段 1 8 からの応答 2 3 4 を受け取った制御手段 1 6 は、処理 1 3 3 においてそのユーザ情報の登録要求 2 3 5 をユーザ情報管理手段 2 0 に発行する。ユーザ情報登録要求 2 3 5 を受け取ったユーザ情報管理手段 2 0 は、処理 1 3 4 においてそれをユーザ情報テーブル 2 1 に登録し、その項目のアドレスを制御手段 1 6 に応答する(2 3 6)。ユーザ情報テーブル 2 1 の当該ユーザ情報を格納した項目のアドレスを受け取った制御手段 1 6 は、処理 1 3 5 においてそのアドレスとユーザ認証情報をユーザ認証情報登録要求 2 3 7 としてユーザ認証情報管理手段 1 7 に発行する。ユーザ認証情報登録要求 2 3 7 を受け取ったユーザ認証情報管理手段 1 7 は、まず処理 1 1 0 においてユーザ認証情報識別子を生成し、処理 1 3 6 においてそれとユーザ認証情報とアクセス時刻とユーザ情報テーブルアドレスとをユーザ認証情報テーブル 1 9 に格納する。それ以降の処理は第 1 の実施例のログイン時の処理の流れと同じである。

【0 0 5 4】以上のようにしてログイン時にユーザ情報を登録する。次に以上のようにして登録したユーザ情報を使用する際の処理の流れをユーザ情報取得の処理の流れを説明する図である図 1 0 を用いて説明する。

【0 0 5 5】まず WWW ゲートウェイ本体部 1 2 のゲートウェイ制御手段 8 から、処理 1 4 1 においてユーザ情報要求 2 4 1 が発行される。ユーザ情報要求 2 4 1 はユーザ管理デーモン通信手段 1 4 の処理 1 0 4 においてユーザ管理デーモン 1 3 へのメッセージ 2 0 4 に変換され発行される。メッセージ 2 0 4 はユーザ管理デーモン 1 3 の WWW ゲートウェイ通信手段 1 5 の処理 1 0 5 において受信、解釈されて制御手段 1 6 に転送される(2 4 2)。制御手段 1 6 では、まず処理 1 4 2 においてメッセージ解析結果 2 4 2 からユーザ認証情報識別子を切り出し、それを基にユーザ情報テーブルアドレス要求 2 4 3 をユーザ認証情報管理手段 1 7 に発行する。ユーザ認証情報管理手段 1 7 は、処理 1 4 3 においてユーザ情報テーブルアドレス要求 2 4 3 に含まれるユーザ認証情報

識別子をキーにユーザ認証情報テーブル 1 9 から当該ユーザのユーザ情報テーブルアドレスを取得し、それを制御手段 1 6 に応答する(2 4 4)。

【0 0 5 6】例えば、図 7 のユーザ認証テーブル 1 9 の例において、ユーザ認証情報識別子として K U I 0 3 8 9 0 V 0 9 3 が与えられたとすると、それに対応したユーザ情報テーブルアドレス: 6 B 7 C 1 1 4 0 が応答される。制御手段 1 6 は、処理 1 4 4 において応答 2 4 4 からユーザ情報テーブルアドレスを切り出しユーザ情報要求 2 4 5 を生成して、それをユーザ情報管理手段 2 0 に発行する。ユーザ情報要求 2 4 5 を受け取ったユーザ情報管理手段 2 0 は処理 1 4 5 においてユーザ情報テーブルアドレスを基にユーザ情報テーブル 2 1 からユーザ情報を取得し、それを制御手段 1 6 に応答する(2 4 6)。

【0 0 5 7】例えば図 8 のユーザ情報テーブル 2 1 の例において、ユーザ情報テーブルアドレス: 6 B 7 C 1 1 4 0 に対応したパラメタ 1: Y Y Y とパラメタ 2: D E F が応答される。応答 2 4 6 を受け取った制御手段 1 6 はそれを WWW ゲートウェイ通信手段 1 5 と WWW ゲートウェイ本体部 1 2 のユーザ管理デーモン通信手段 1 4 を経由してゲートウェイ制御手段 8 に応答する。以上により WWW ゲートウェイ本体部 1 2 でユーザ情報を取得でき、以降でユーザ情報を使った処理を実行できる。

【0 0 5 8】ログアウト時およびタイムアウト時にユーザ認証情報テーブル 1 9 の当該ユーザの項目が削除されるタイミングで、ユーザ情報テーブル 2 1 の当該ユーザの項目も削除する。

【0 0 5 9】以上のようにユーザ管理デーモン 1 3 にユーザ情報テーブル 2 1 を設けそこにユーザ固有の追加情報を格納して、ユーザ情報管理手段 2 0 でそれを管理することにより、画面間でユーザ固有の追加情報を継承することが可能となる。これは、画面情報に埋め込んで継承した場合、WWW ブラウザ 4 の機能により埋め込んだ情報が参照できてしまうためセキュリティ上問題があるようなユーザ情報の継承において特に有効である。

【0 0 6 0】次に第 3 の実施例について説明する。

【0 0 6 1】第 1 の実施例において、タイムアウトによってユーザ認証情報テーブルから登録を削除されたユーザが WWW ゲートウェイシステムにアクセスしたとき、WWW ゲートウェイシステムは当該ユーザにタイムアウトで登録が削除されていることを通知し、再ログインするためにユーザ認証画面を表示する。しかし、この手順で再ログインすると当該ユーザがタイムアウト以前に行ってきた操作は全て無効になり、もう一度最初から操作を繰り返さなければならないという問題がある。そこで本実施例では、タイムアウト時に表示するユーザ認証画面の画面情報に当該ユーザがタイムアウト前の操作を継続するための情報(以下では継続処理情報と呼ぶ)を埋め込むことで、ユーザ認証画面から再ログインすると

タイムアウト前の操作以降の処理を継続して行うことができるWWWゲートウェイシステムについて説明する。

【0062】図11は本実施例の構成を示すブロック図である。図において、WWWゲートウェイ本体部12に継続処理情報埋め込み手段22を追加する。

【0063】本実施例の処理ではまず当該ユーザのユーザ認証情報識別子がユーザ認証情報テーブルになかった場合の再ログインのためのユーザ認証画面に継続処理情報を埋め込む処理を行っておき、再ログインのためのユーザ認証画面からユーザ認証情報を入力し認証に成功した後、継続処理情報に従って処理を継続する。

【0064】図12は本実施例における再ログインのためのユーザ認証画面生成処理の流れを説明するための図である。第1の実施例で説明した既存システムの処理をWWWゲートウェイシステム7から行うときの処理(図5)において、ユーザ認証情報管理手段17の処理123で、ユーザ認証情報識別子に対応したユーザ認証情報がユーザ認証情報テーブル19に存在しない場合、ユーザ認証情報管理手段17はエラーを制御手段16に渡し、制御手段16はそれをWWWゲートウェイ通信手段15とWWWゲートウェイ本体部12のユーザ管理デーモン通信手段14を経由してゲートウェイ制御手段8に応答する(251)。エラー応答251を受けたゲートウェイ制御手段8は、処理151において再ログインのためのユーザ認証画面の出力要求252を発行する。

【0065】第1の実施例のシステムでは再ログインのためのユーザ認証画面出力要求252を他の画面出力要求と同様にHTML生成・出力手段11が処理する。それに対して本実施例では、再ログインのためのユーザ認証画面出力要求252は、まず継続処理情報埋め込み手段22が処理する。再ログインのためのユーザ認証画面出力要求252を受け取った継続処理情報埋め込み手段22は、処理152において今回ユーザが行おうとした操作に関するパラメタ(パラメタ解析手段9が解析したもの)を画面情報に埋め込める形にしてそれをHTML生成・出力手段11に渡す(253)。画面情報に埋め込める形としては、HTMLのhiddenタグを使用する。

【0066】HTML生成・出力手段11は、処理116において継続処理情報253を埋め込んだ画面情報を生成し、処理117においてそれをWWWサーバ5に出力する。以上の手順でタイムアウト前の操作を継続するための継続処理情報を埋め込んだ再ログインのためのユーザ認証画面を表示する。

【0067】次に再ログインのためのユーザ認証画面でユーザがログインしたときの処理の流れを図13を用いて説明する。第1の実施例で説明したログイン時の処理(図4)において、ユーザ認証情報管理手段17がユーザ認証情報をユーザ認証情報テーブルに格納し、その結果としてユーザ認証情報識別子を制御手段16に応答す

る。ユーザ認証情報識別子を受け取った制御手段16は、それをWWWゲートウェイ通信手段15とWWWゲートウェイ本体部12のユーザ管理デーモン通信手段14を経由してゲートウェイ制御手段8に応答する。ユーザ認証識別子を受け取ったゲートウェイ制御手段8は、処理124において再ログインのためのユーザ認証画面に埋め込まれていた継続処理情報を基に既存システム6に処理要求224を発行する。処理要求224は、既存システム通信手段10が処理125において既存システム6向けの処理要求225に変換して既存システム6に発行する。以下、既存システム6で処理を実行した以降の処理の流れは、従来のWWWゲートウェイシステムと同様である。

【0068】以上のように、WWWゲートウェイ本体部12に継続処理情報埋め込み手段22を追加して再ログインのためのユーザ認証画面の画面情報に継続処理情報を埋め込み、再ログイン時の処理のユーザ認証情報のユーザ認証情報テーブル19への格納後にその継続処理情報に従った処理を実行することにより、タイムアウトによってユーザ認証情報テーブルから登録を削除されたユーザがWWWゲートウェイシステムにアクセスしたとき、最初から処理をやり直すことなく、タイムアウト前の処理を継続することが可能となる。

【0069】

【発明の効果】ユーザ認証によるアクセス管理を行う既存システムに対するWWWゲートウェイシステムに関して、ユーザ認証情報を計算機環境に常駐しているユーザ管理デーモンに管理させ、WWWゲートウェイ本体部はそこから取得したユーザ認証情報を既存システムに渡すことにより、既存システムのアクセス管理をそのまま活用したユーザ認証を行うことが可能となる。その際、ユーザの入力したユーザ認証情報に基づいて複数の画面を遷移して操作を行うような処理において、ユーザ認証情報の画面間の継承が問題となるが、ユーザ管理デーモンがユーザ認証情報を管理したまま計算機環境に常駐し続け、ユーザ認証情報にアクセスするためのユーザ認証情報識別子(ユニークかつハッキングされる恐れのない識別子)で画面間の継承を行うことにより、セキュリティとユーザの利便性の両方を確保することが可能となる。

【0070】また、ユーザ管理デーモンにユーザ情報テーブルを設け、各ユーザ固有のデータを管理することにより、従来画面情報に埋め込んで管理するしかなかったユーザデータを画面情報に埋め込むことなく画面間で継承することが可能となる。

【0071】さらに、ユーザが接続断通知をすることなくWWWゲートウェイシステムへのアクセスを終了するなどによりユーザ認証情報テーブルが過大となることを防ぐために、ユーザ管理デーモンはユーザ認証情報テーブルの最終アクセス時刻をチェックし、それが予め定められた有効期間を経過している場合には当該ユーザのユ

ーザ認証情報をユーザ認証情報テーブルから削除するが、ユーザ認証情報削除後にWWWゲートウェイシステムにアクセスした際に表示するユーザ認証画面に前回の操作から継続して処理を実行するための情報を埋め込むことにより、ユーザ認証後操作を始めからやりなおすことなく直前の操作から継続して処理することが可能となる。

【図面の簡単な説明】

【図 1】第 1 の実施例における構成を表すブロック図である。

【図 2】従来のWWWゲートウェイシステムの構成を説明するための図である。

【図 3】ユーザ認証情報テーブルの例を説明するための図である。

【図 4】ログイン時の処理の流れを説明するための図である

【図 5】WWWゲートウェイシステムから既存システムの処理を実行するときの処理の流れを説明するための図である。

【図 6】第 2 の実施例における構成を表すブロック図である。

【図 7】第 2 の実施例におけるユーザ認証情報テーブルの例を説明するための図である。

【図 8】ユーザ情報テーブル 2 1 の例を説明するための図である。

【図 9】第 2 の実施例におけるログイン時の処理の流れを説明するための図である。

【図 1 0】第 2 の実施例におけるユーザ情報取得処理の流れを説明するための図である。

【図 1 1】第 3 の実施例における構成を表すブロック図 30

である。

【図 1 2】第 3 の実施例における再ログインのためのユーザ認証画面生成処理の流れを説明するための図である。

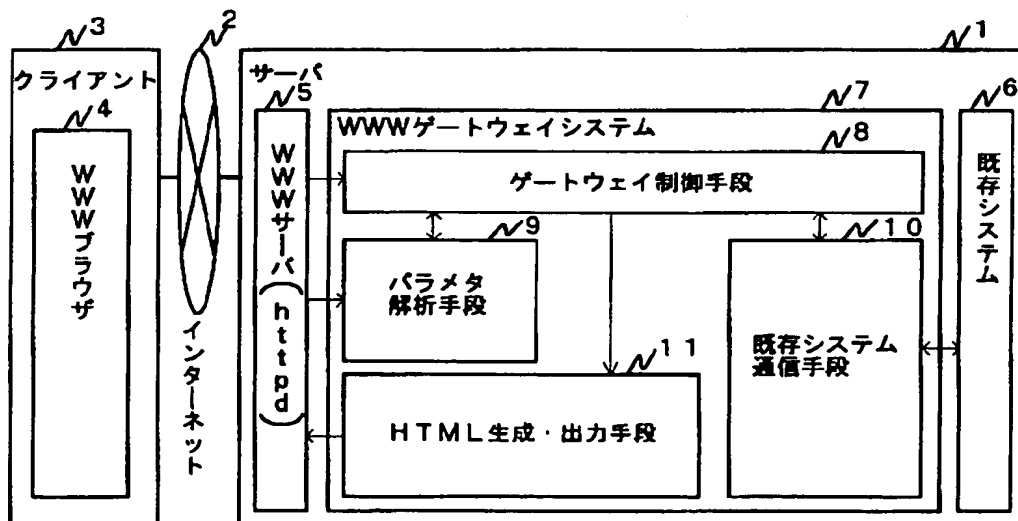
【図 1 3】第 3 の実施例における再ログイン時の処理の流れを説明するための図である。

【符号の説明】

- 1・・・サーバ、
- 2・・・インターネット、
- 3・・・クライアント、
- 4・・・WWWブラウザ、
- 5・・・WWWサーバ、
- 6・・・既存システム、
- 7・・・WWWゲートウェイシステム、
- 8・・・ゲートウェイ制御手段、
- 9・・・パラメタ解析手段、
- 10・・・既存システム通信手段、
- 11・・・HTML生成・出力手段、
- 12・・・WWWゲートウェイ本体部、
- 13・・・ユーザ管理デーモン、
- 14・・・ユーザ管理デーモン通信手段、
- 15・・・WWWゲートウェイ通信手段、
- 16・・・制御手段、
- 17・・・ユーザ認証情報管理手段、
- 18・・・既存システム問合わせ手段、
- 19・・・ユーザ認証情報テーブル、
- 20・・・ユーザ情報管理手段、
- 21・・・ユーザ情報テーブル、
- 22・・・継続処理情報埋め込み手段

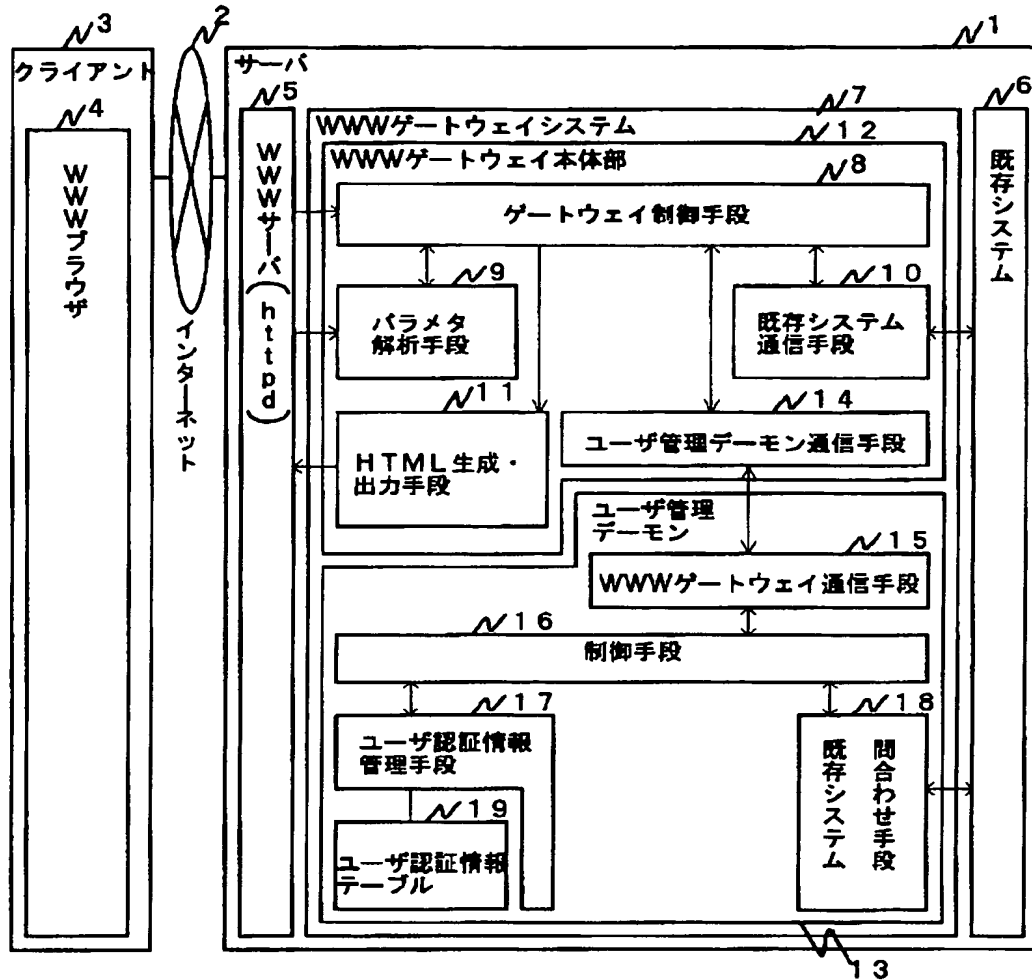
【図 2】

図 2



【図 1】

図 1



【図 3】

図 3

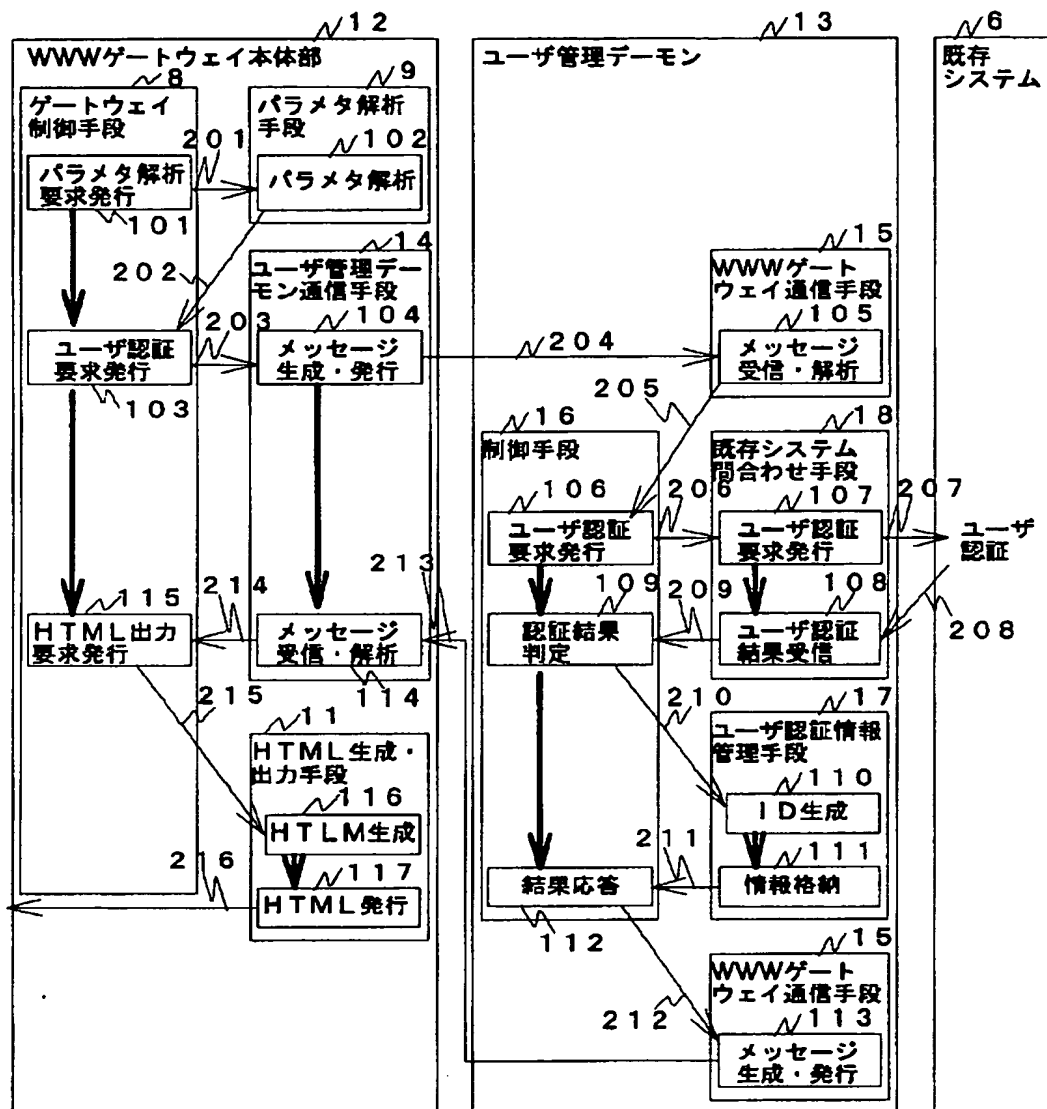
ユーザ認証情報識別子	ユーザID	パスワード	IPアドレス	最終アクセス時刻
97827ABC3228W	AIHARA	888JBN7V	123.45.67.890	980308170532
KU103980V093	AIKOU	ZZZAA00	123.45.67.123	980308154717
OPK99UYV7Y5C	AKIYAMA	888JBN7V	123.45.12.345	980308105908

【図 7】

図 7

ユーザ認証情報識別子	ユーザID	パスワード	IPアドレス	最終アクセス時刻	ユーザ情報テーブル
97827ABC3228W	AIHARA	888JBN7V	123.45.67.890	980308170532	887C1100
KU103980V093	AIKOU	ZZZAA00	123.45.67.123	980308154717	887C1140
OPK99UYV7Y5C	AKIYAMA	888JBN7V	123.45.12.345	980308105908	887C1180

图 4

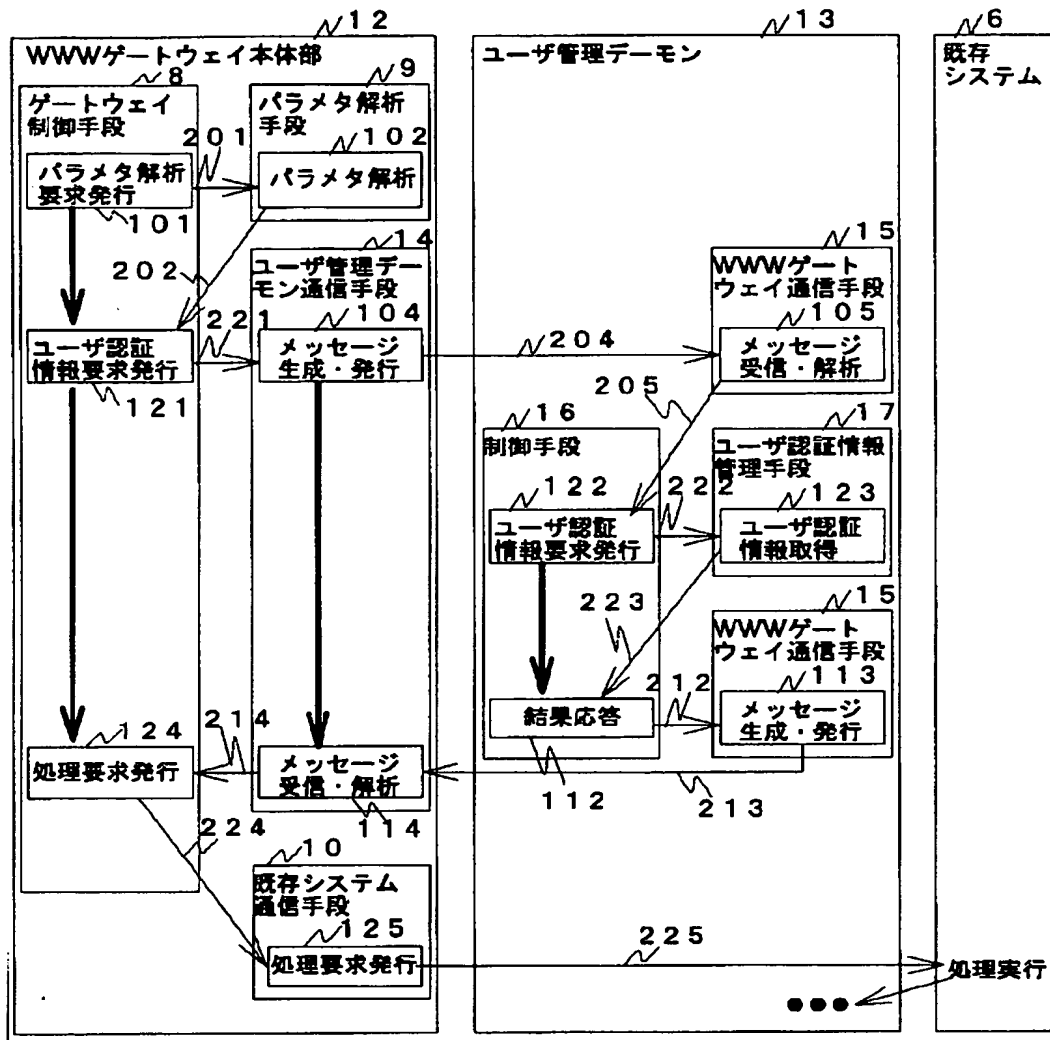


アドレス N21

	パラメタ1	パラメタ2
687C1100	XXX	ABO
687C1140	YYY	DEF
687C1180	ZZZ	GHI
	...	

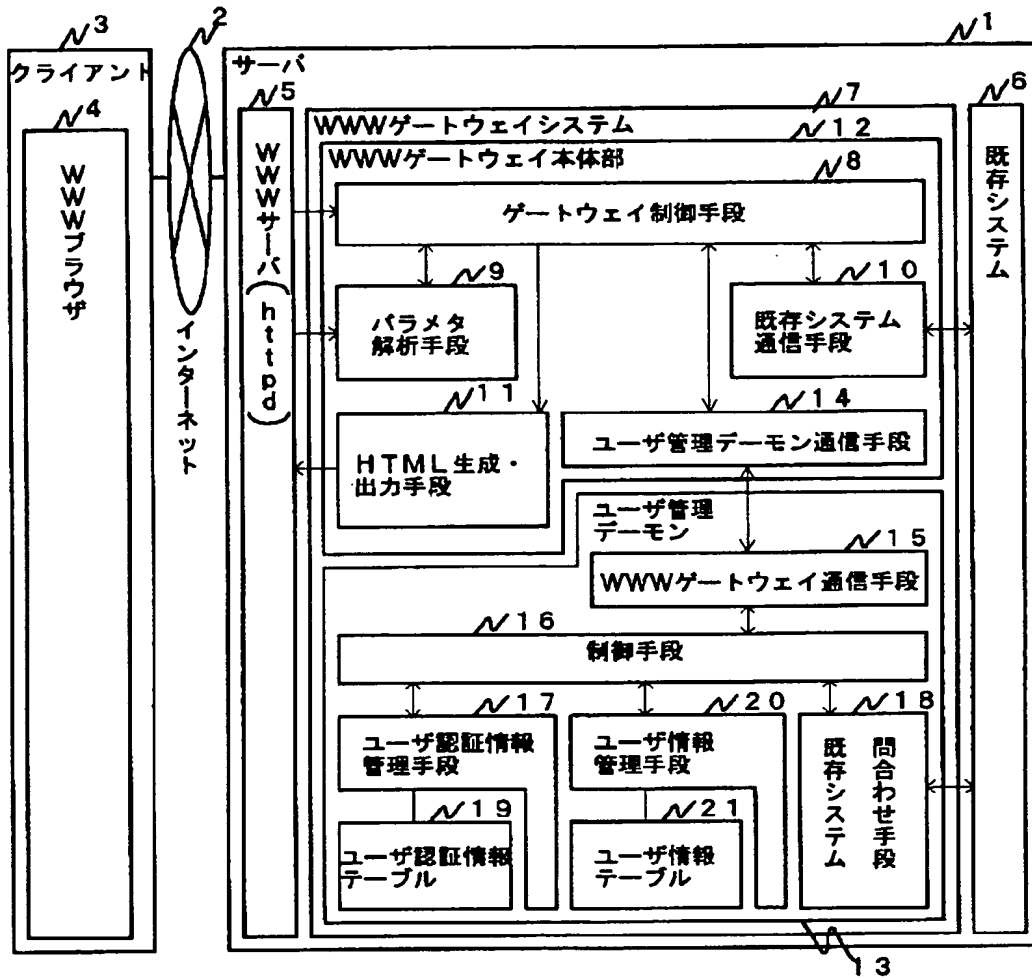
【図5】

図5



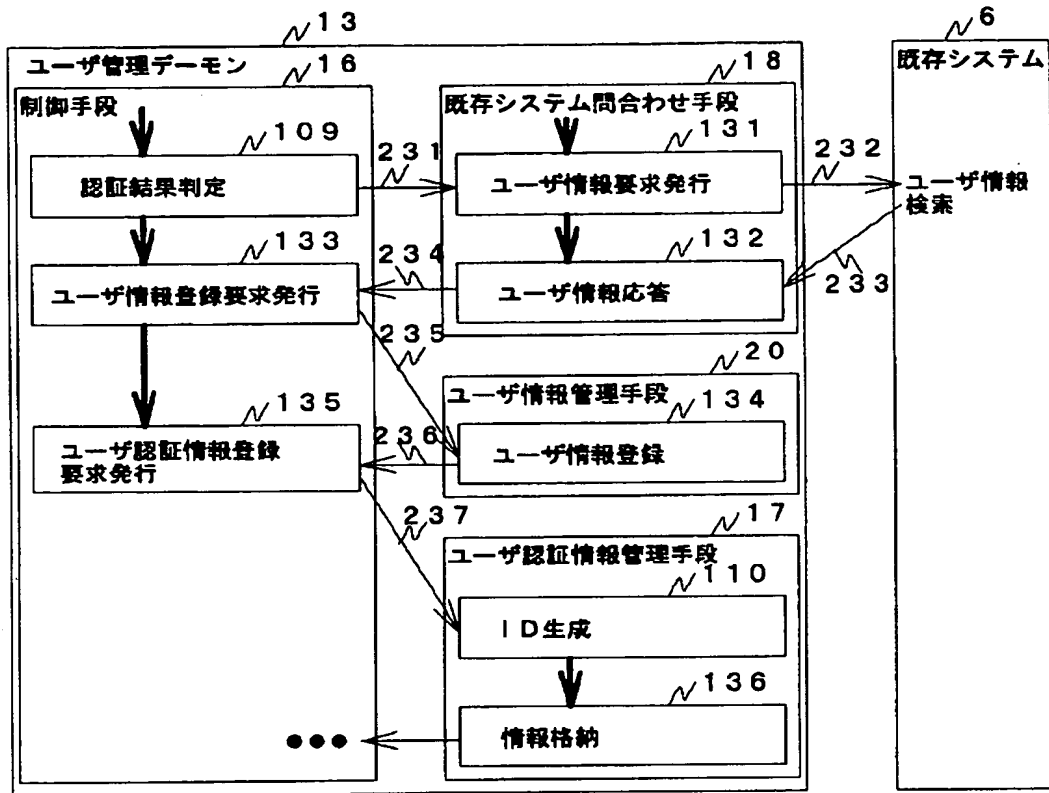
【図6】

図6



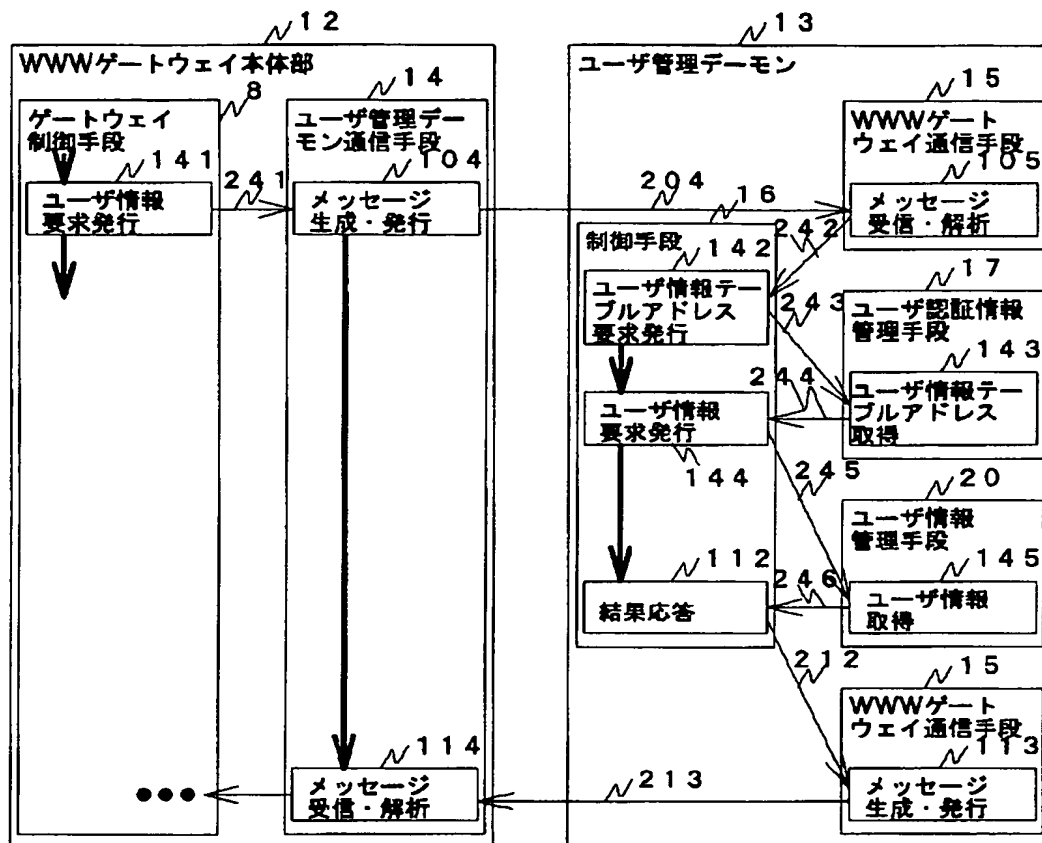
【図9】

図9



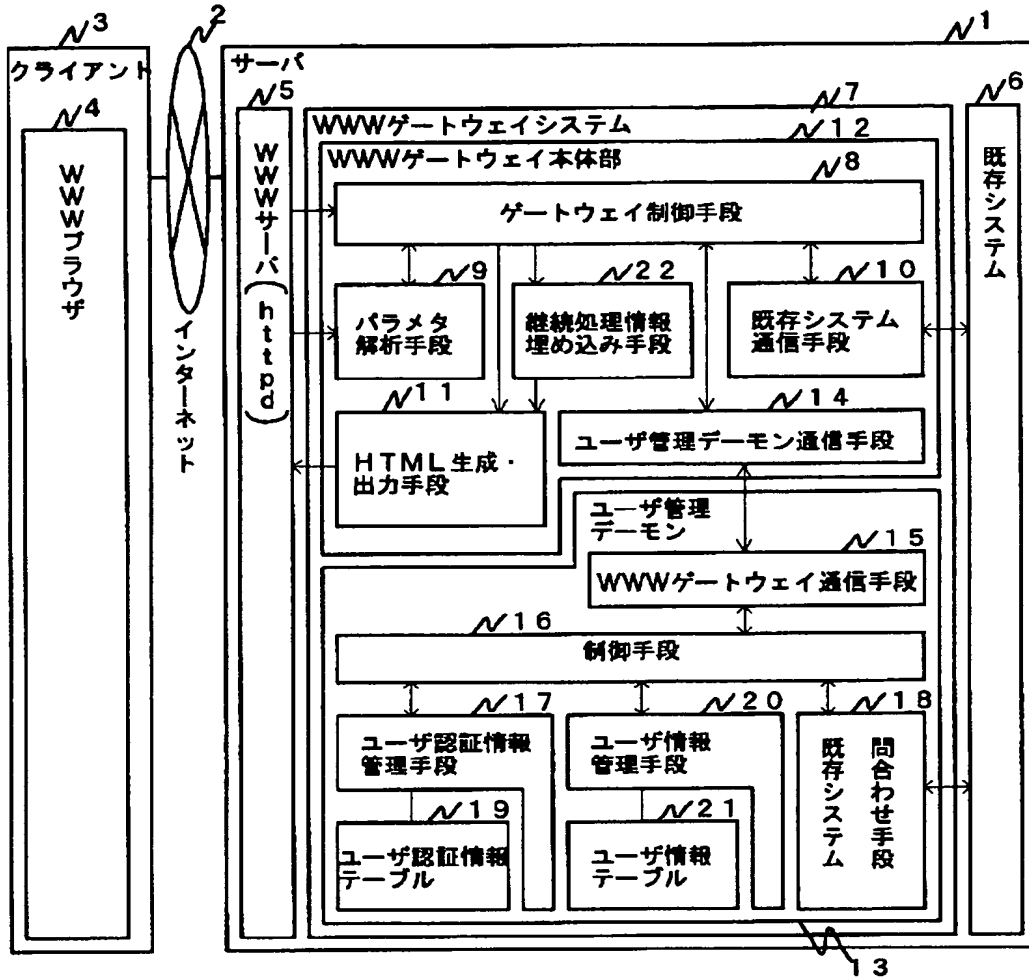
【図10】

図10



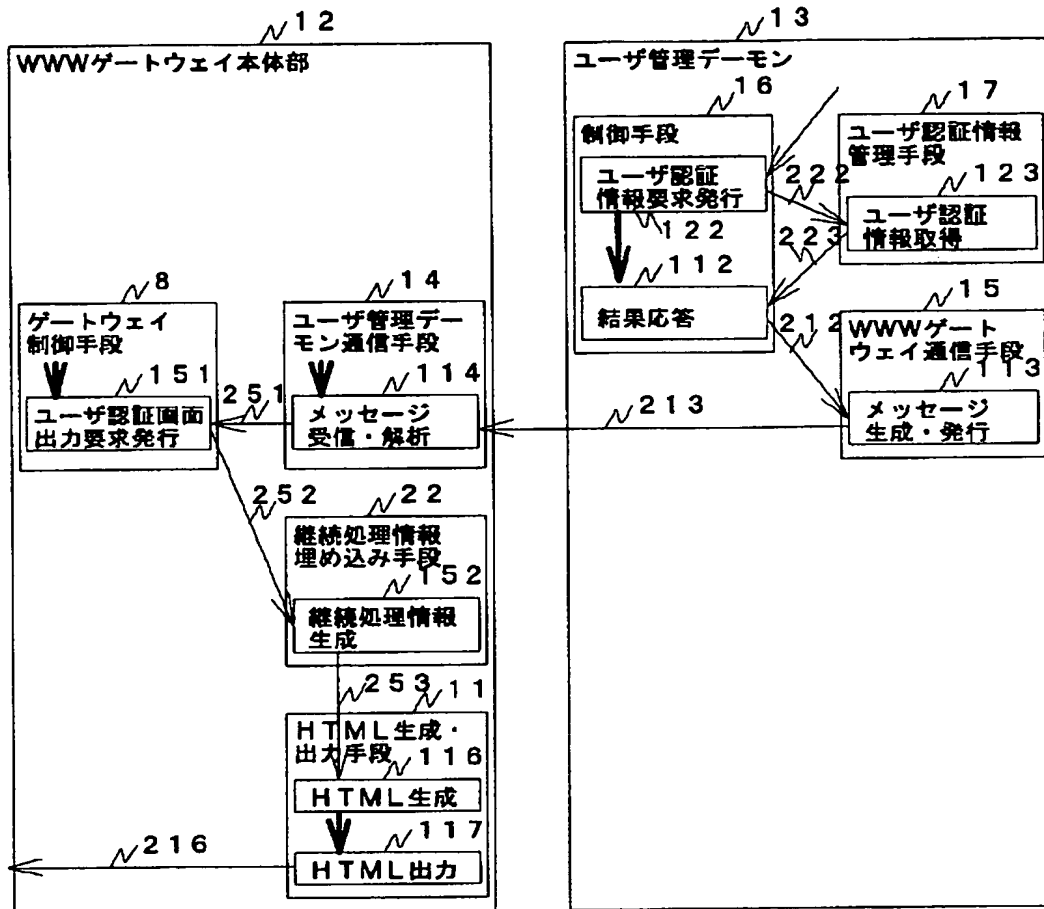
【図11】

図11



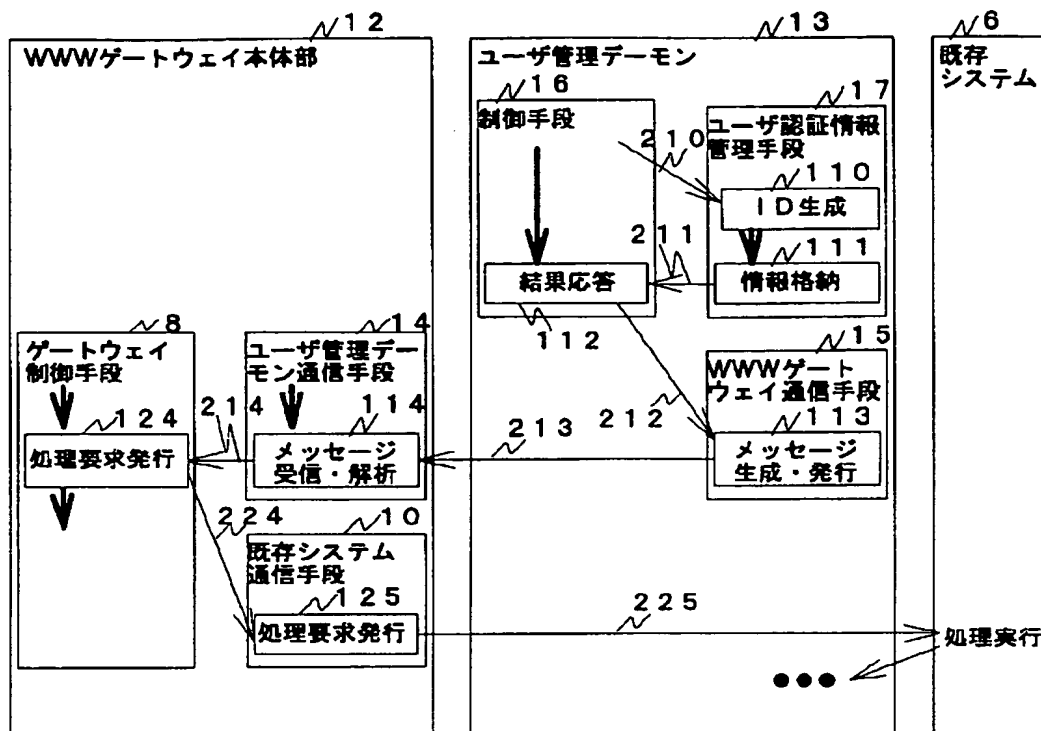
【図 12】

図 12



【図 13】

図 13



フロントページの続き

(72) 発明者 大北 龍太郎
 大阪府大阪市中央区北浜三丁目 5 番 29 号
 日立西部ソフトウェア株式会社内

(72) 発明者 大野 広宣
 大阪府大阪市中央区北浜三丁目 5 番 29 号
 日立西部ソフトウェア株式会社内

(72) 発明者 林 龍介
 大阪府大阪市中央区北浜三丁目 5 番 29 号
 日立西部ソフトウェア株式会社内

(72) 発明者 多田 勝己
 神奈川県川崎市幸区鹿島田 890 番地の 12
 株式会社日立製作所情報・通信開発本部内